Amendments to the Claims

Claim 1. (currently amended) A machine readable medium that provides instructions, which when executed by at least one processor, cause said processor to perform operations comprising:

decrypting a payload of a data block received from a protocol-specific device;

encrypting the [[a]] payload of a data block of a data-stream with at least one key, before transmitting the data-stream from a first system to a second system, wherein the first system comprises a protected content exchange (PCX) module, and wherein the second system comprises at least one application decoder module;

replacing a portion of said payload with a tag that identifies an at least one decrypting key to said first system, before said transmitting; and

setting a flag in a header of the data block that indicates that said payload has said tag, before said transmitting.

Claim 2. (original) The medium defined in claim 1 wherein said encrypting includes encrypting said portion of said payload.

Claim 3 (currently amended) The medium defined in claim 1 wherein said tag includes one of:

a data-stream identifier having sufficient information to access said at least one key, and

a data-stream identifier having insufficient information to access said at least one key, and a source stream identifier, said source stream identifier comprising a source of said keys, and [[if]] when necessary to provide sufficient information to access said at least one key, a source of said portion of said payload.

Claim 4. (previously presented) The medium defined in claim 1 wherein said operations further include

receiving a transmission from said second system that includes data indicating said tag; and

sending said keys, and if necessary, said portion of said payload, to said second system based on said transmission.

Claim 5. (previously presented) The medium defined in claim 1 wherein said operations further include before setting said flag and encrypting said payload; said first system

receiving a stream of data from a third system wherein said data-stream is based on said stream of data, and wherein said third system is a source device.

Claim 6. (currently amended) A machine readable medium that provides instructions, which when executed by at least one processor, cause said processor to perform operations comprising:

after a fixed-length data block of a data-stream, the data block having both a payload including an encrypted data portion and at least one tag bits, and a header, is received by a second system, reading a flag in the header indicating that the data block has the tag bits, wherein a segment of the payload is removed by a transmitting first system when necessary to accommodate the at least one tag bit before the data block is received by the second system, wherein the encrypted data portion comprises at least one data portion comprising an encrypted data block of a first decrypted data block, the first decrypted data block being a data block decrypted by the first system before transmission from the first system to the second system;

if the flag indicates that the data block has the tag bits, reading at least one bit identifying the data-stream in the tag bits;

sending a datum from the second system to the transmitting first system indicating an identification of the read data-stream based on the at least one bit;

the second system receiving from the first system a definition of a decrypting keys for the data-stream based on the datum sent from the second system to the first system; and

decrypting the data block in the second system based on the decrypting keys received by the second system.

Claim 7. (previously presented) The medium defined in claim 6 further including the second system receiving from the first system the removed segment of the payload based on the datum sent from the second system to the first system.

Claim 8. (previously presented) The medium defined in claim 7 further including the second system replacing the at least one tag bits in the payload with the removed segment of the payload, and if the removed segment of the payload is encrypted then decrypting includes decrypting the removed segment of the payload.

Claim 9. (currently amended) A method comprising:

a sending system replacing a portion of a decrypted data block payload with at least one tag bits that identify an at least one decrypting key;

said sending system setting a flag in a header of said data block that indicates at least one of said payload is encrypted and said payload includes said tag;

said sending system encrypting said payload with at least one key; and

said sending system transmitting said data block to a receiving system after said setting a flag, said encrypting, and said replacing,

wherein the sending system comprises a protected content exchange (PCX) module, and wherein the receiving system comprises at least one application decoder module.

Claim 10. (original) The method defined in claim 9 wherein said encrypting includes encrypting said payload portion.

Claim 11. (currently amended) The method defined in claim 9 further including said sending system transferring a first data characterized by:

said at least one key to said receiving system; and

~~if necessary ,~~ said replaced payload portion to said receiving system.

Claim 12. (original) The method defined in claim 11 wherein said sending system transmitting said first data is based upon said receiving system transmitting to said sending system said tag bits.

Claim 13. (previously presented) The method defined in claim 12 further including one of:

(a) said sending system transmitting said replaced payload portion to said receiving system based upon said receiving system transmitting to said sending system said tag bits; and said receiving system replacing said tag bits with said replaced payload portion in response to receiving said replaced payload portion from said sending system, and wherein said encrypting includes encrypting said replaced payload portion, and said decrypting includes decrypting said replaced payload portion; and

(b) said sending system transmitting said replaced payload portion to said receiving system based upon said receiving system transmitting to said sending system a first datum that identifies a data-stream that includes said data block, and said receiving system replacing said payload portion in response to receiving said replaced payload portion from said sending system.

Claim 14. (original) The method defined in claim 9 wherein said transmitting occurs via a shared memory unit.

Claim 15. (original) The method defined in claim 9 wherein

said sending system and said receiving system are separate physical devices;

said transmitting of said data block occurs on a first channel; and

transmitting of non-data block data including at least one of said key from said sending system to said receiving system, said payload portion from said sending system to said receiving system, and a datum that identifies a data-stream that includes said data block, occurs on at least one separate second channel.

Claim 16. (original) The method defined in claim 9 wherein said tag bits further identify a source of said keys in said sending system.

Claim 17. (currently amended) A method comprising:

a receiving system of an encrypted data block that has a payload and a header reading a set flag in a header of said data block;

said receiving system reading at least one tag bit in a payload portion of said data block in response to said reading said set flag;

said receiving system sending a first datum to a sending system of said encrypted data block that identifies a data-stream that includes said data block based on said read tag bits; and

said receiving system decrypting a payload data of said payload portion in response to receiving a decryption keys from said sending system,

wherein the sending system comprises a protected content exchange (PCX) module, the sending system to decrypt an initial data block and to encrypt at least a portion of the decrypted initial data block prior to sending the encrypted data block that has a payload and header to the receiving system, and wherein the receiving system comprises at least one application decoder module.

Claim 18. (original) The method defined in claim 17 wherein said tag bits have a source identifier in said sending system of said decryption keys, and further including said receiving system sending said source identifier to said sending system in response to said reading.

Claim 19. (currently amended) A data safeguarding system for a data block sent from a first system to a second system including:

a first system payload replacement circuit that replaces a portion of a payload of said data block with a tag data that indicates at least one decryption key for said data block in said first system, wherein the first system payload replacement circuit decrypts said payload prior to replacement of the portion of the payload;

a first system header flag setting circuit that sets a flag in a header of said data block when said data block includes said tag;

a first system encryption circuit that encrypts said decrypted payload ~~with~~ using said at least one decryption key; and

a first system data-stream sending circuit that sends a data-stream that includes said data block to said second system after said header flag setting circuit sets said flag and said encryption circuit encrypts said payload and said payload replacement circuit replaces said portion of a payload, wherein the first system comprises a protected content exchange (PCX) module, and wherein the second system comprises at least one application decoder module.

Claim 20. (original) The system defined in claim 19 wherein said first system encryption circuit encrypts said portion of said payload.

Claim 21. (currently amended) The system defined in claim 19 further including a first system sending circuit that sends said at least one key to said second system, wherein the first system sending circuit sends~~, if necessary,~~ said portion of said payload to said second system.

Claim 22. (original) The system defined in claim 21 wherein said first system sending circuit sending is based upon said first system receiving from said second system a first datum that indicates at least one decryption key for said data block in said first system

Claim 23. (previously presented) The system defined in claim 19, further including:

a second system header flag reading circuit that reads said flag in said header;

a second system tag data reading circuit that reads said tag data if said second system header flag reading circuit indicates that said flag includes said tag data;

a second system data sending circuit that sends to said first system a datum that identifies said data-stream based on said tag data; and

a second system decrypting circuit that decrypts said encrypted payload.

Claim 24. (original) The system defined in claim 23 further including a first system key sending circuit that sends said at least one key to said second system, and wherein said second system decrypting circuit decrypts said data stream based on said at least one key.

Claim 25. (previously presented) The system defined in claim 23 further including

a first system sending circuit that sends said replaced portion of said payload to said second system in response to receiving from said second system a datum that indicates said decryption keys in said first system

said first circuit encryption circuit further encrypts said replaced portion of said payload;

a second system payload replacement circuit that replaces said received tag data with said replaced portion of said payload; and

said second system decrypting circuit further decrypts said replaced portion of said payload.

Claim 26. (original) The system defined in claim 19 wherein at least one of:

said sending occurs via a shared memory; and

said first system and said second system are separate physical devices; said sending of said data-stream occurs on a first channel; and sending non-data-stream data including at least one of said at least one key, said portion of said payload, and said data-stream identifier occurs on a second channel.

Claim 27. (original) The system defined in claim 23 wherein said tag data further has an identifier for accessing a first system unit that can send to said second system said keys.

Claim 28. (currently amended) The system defined in claim 19 further including before said first circuit header flag setting circuit setting said flag and said first circuit encryption circuit encrypting said payload, a second circuit receiving circuit that can receive a stream of data from a third system wherein said data-stream is based on said stream of data, wherein said third system comprises a source device, and wherein a first data block of the received data stream is to be sent to a different one of the at least one application decoder module than a second data block of the received data stream.

Claim 29. (currently amended) A system for safeguarding a data block of a data-stream sent from a first system to a second system comprising:

a second system header flag reading circuit that reads a flag in a header of said data block;

a second system tag data reading circuit that reads a data-stream identifier in a tag data of a payload portion of said block if said header flag reading circuit indicates that said flag includes said tag data; and

a second system data sending circuit that sends to said first system a first datum that identifies said data-stream based on said data-stream identifier,

wherein the first system comprises a protected content exchange (PCX) module, and wherein the second system comprises at least one application decoder module, the PCX module to decrypt an initial data block and to encrypt at least a portion of the decrypted initial data block prior to sending the encrypted data block that has a payload and header to the at least one application decoder module.

Claim 30. (original) The system defined in claim 29 further including a second system decrypting circuit that decrypts said data block.

Claim 31. (withdrawn) A method comprising:

receiving a data stream from a source device, by a sending system, the data stream comprising a sequence of data blocks, wherein each data block comprises a header and a payload;

the sending system negotiating with each of at least one application decoder to generate a session key shared between the sending system and the at least one application decoder, each session key to encrypt at least a decryption key;

for each data block, encrypting a payload by the sending system, the payload corresponding to the each data block, the encryption using at least one key;

the sending system storing a portion of the encrypted payload to be transmitted later to the application decoder, wherein the stored portion is one of an encrypted portion and an unencrypted portion;

the sending system replacing the stored portion of the encrypted payload with a tag, the tag identifying the data stream and a source of the data stream;

the sending system setting a flag in a header of the data block corresponsing to the encrypted payload, the flag indicating that (a) at least one of said payload is encrypted and (b) said payload includes the tag; and

transmitting by the sending system each of the data blocks to an appropriate one of the at least one application decoder.

Claim 32. (withdrawn) The method as recited in claim 31, wherein the sending system comprises a protected content exchange (PCX) module having at least one decryptor, a protocol specific registration engine, at least one encryptor, and a negotiator.

Claim 33. (withdrawn) The method as recited in claim 31, wherein each of the at least one application decoders use a different session key.

Claim 34. (withdrawn) The method as recited in claim 31, wherein the data stream identifier references an encryption key and the saved portion of the payload.

Claim 35. (withdrawn) The method as recited in claim 31, wherein each of the data blocks is transmitted via a first transmission channel and negotiating is via at least one separate second transmission channel.

Claim 36. (withdrawn) The method as recited in claim 35, wherein negotiating from said sending system to said receiving system, comprises transmitting of non-data block information including (a) at least one key selected from the group of session keys, encryption keys and decryption keys, (b) the portion of the encrypted payload to be transmitted later from the sending system to said receiving system, and (c) a datum that identifies a data-stream that includes the data block.

Claim 37. (withdrawn) The method as recited in claim 31, further comprising determining, for each data block, by a device specific driver, to which of the at least one application decoders the data block should be sent based on a protocol specific to the data block.

Claim 38. (withdrawn) A system for safeguarding protocol-specific data within a device, comprising:

a first transmission channel to transmit at least one protocol specific encrypted data stream;

at least one protected content exchange (PCX) device configured to translate the at least one protocol specific encrypted data stream into a PCX encrypted data stream; and

at least one application decoder configured to decode the PCX encrypted data stream, the decoded PCX data stream comprising a plurality of data blocks each data block having a header and a payload,

wherein the at least one PCX device comprises:

at least one protocol specific registration engine configured to register the at least one application decoder,

at least one negotiator configured to negotiate at least one device key for the at least one application decoder, the negotiator using a second transmission channel to communicate non-data block data between the PCX device and the at least one application decoder,

at least one decryptor configured to decrypt the at least one protocol specific encrypted data stream,

at least one encryptor configured to encrypt at least a portion of the decrypted data stream using the at least one device key to produce at least one re-encrypted data stream,

a payload replacement module to replace a portion of a payload of the data block with a tag data that indicates at least one decryption key for the data block in the PCX device,

a header flag setting module that sets a flag in a header of the data block when the data block includes the tag, and

a data-stream sending module that sends a data-stream, the data stream including the data block, to the at least one application decoder after the header flag setting module sets the flag and the encryptor encrypts the data stream and the payload replacement module replaces the portion of a payload.

Claim 39. (new) A machine readable medium that provides instructions, which when executed by at least one processor, cause said processor to perform operations comprising:

decrypting a data block received from a protocol-specific device;

encrypting a portion of a payload of a data block of a data-stream with at least one key, before transmitting the data-stream from a first system to a second system;

replacing the portion of said payload with a tag that identifies an at least one decrypting key to said first system, before said transmitting; and

setting a flag in a header of the data block that indicates that said payload has said tag, before said transmitting.

Claim 40. (new) The medium defined in claim 39 wherein said encrypting includes encrypting said entire payload, including the at least one decrypting key.